Discrete Mathematics 83 (1990) 249–263
North-Holland

ON THE DELSARTE–GOETHALS CODES AND THEIR FORMAL DUALS

Ferdinand B. HERGERT
Siemens AG, Corporate Research and Development, 8000 Munich 83, F.R. Germany

Received 18 December 1987
Revised 3 October 1988

Exploiting properties of association schemes arising from quotient spaces of nested linear codes having the same automorphism group, we show how the the nonlinear Delsarte–Goethals codes can be used to construct their formal duals. This yields a unified construction for these two families of nonlinear codes.

1. Introduction

Besides being the best codes known for their parameters, the Delsarte–Goethals family of codes share the remarkable property that, although nonlinear, they are distance invariant and possess formal duals, i.e. for every Delsarte–Goethals code there exists another nonlinear code which is also distance invariant and whose distance distribution is the MacWilliams transform of the distance distribution of the Delsarte–Goethals code.

This property is best known for a special member of this class, the Kerdock code $K(m)$ [6], which using the notation given in Theorem 1 below, is a $\mathrm{DG}(m, \frac{1}{2}m)$-code. $K(m)$ has as its formal dual the Preparata code $P(m)$ [8], [1]. Another example is Goethals' generalization of the Preparata code [5], which is the formal dual of $\mathrm{DG}(m, \frac{1}{2}m - 1)$.

The following theorem [3] collects some of the properties of the DG-codes:

Theorem 1 (Delsarte–Goethals). *For even $m = 2t \geqslant 4$ and $1 \leqslant d \leqslant \frac{1}{2}m$ there exists a Delsarte–Goethals code* $\mathrm{DG}(m, d)$ *of length 2^m, containing 2^k codewords, where $k = (m-1)(t-d+1)+m+1$, having minimum distance $2^{m-1} - 2^{m-1-d}$.*

For $d = 1$, $\mathrm{DG}(m, d)$ *is the second order Reed–Muller code* $\mathrm{RM}(2, m)$, *while for $2 \leqslant d \leqslant \frac{1}{2}m$,* $\mathrm{DG}(m, d)$ *is a nonlinear subcode of* $\mathrm{RM}(2, m)$, *consisting of a union of cosets of* $\mathrm{RM}(1, m)$. $\mathrm{DG}(m, \frac{1}{2}m)$ *is the Kerdock code $K(m)$.*

Since every $\mathrm{DG}(m, d)$ code has a formal dual, we are faced with two families of nonlinear codes, the DG-codes and their formal duals, which we shall denote as GD-codes. The GD-codes contain as members the Preparata code and Goethals' generalization of the Preparata code. Although the two families are

formal duals of each other, their definitions and constructions seem to be quite unrelated.

What we will show in this paper is a simple link between these codes. Their constructions are essentially identical, i.e. given the family of DG(m, d)-codes for a fixed m, we can use these codes in a simple way to directly construct the dual family and vice versa.

We will prove the theorem:

Theorem 2. *For m and d as in Theorem 1 there exists a distance invariant code* GD(m, d), *whose distance distribution is the MacWilliams transform of the distance distribution of the Delsarte–Goethals code* DG(m, j) *where* $j + d = \frac{1}{2}m + 2$. *Furthermore there exists a linear bijection α (to be defined later)*

$$\alpha : F_2^{2^m} \to F_2^{2^m}$$

with the following property:
Let DG(m, d) *be the union of cosets of* RM(1, m) *in* RM(2, m) *with coset representatives*

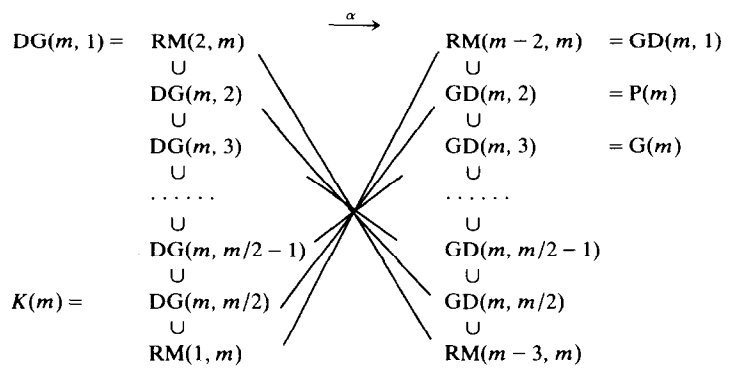
$$a_0, a_1, \cdots a_s \in F_2^{2^m},$$

then the code GD(m, d) *is the union of cosets of* RM($m-3$, m) *in* RM($m-2$, m) *with coset representatives*

$$\alpha(a_0), \alpha(a_1), \cdots \alpha(a_s) \in F_2^{2^m}.$$

For $d = 1$, GD(m, 1) *is the Reed–Muller code* RM($m-2$, m), *while for $2 \leqslant d \leqslant \frac{1}{2}m$,* GD($m$, d) *is a nonlinear subcode of* RM($m-2$, m). *The Preparata code and Goethals' generalization of the Preparata code $G(m)$ are members of this family,* GD(m, 2) *and* GD(m, 3) *respectively.*

The following table illustrates the situation. (Formal) duals are connected by a line. The mapping α relates the codes on the left side to the codes on the right side of the table as described above.



To prove Theorem 2 we will make use of duality properties of association schemes on quotient spaces of nested linear codes $B \subset A \subset F_2^n$ induced by the action of a common automorphism group of the codes A and B. Therefore we must first study these schemes in a general setting.

2. Linear association schemes

We shall use the notation of [7, Ch. 21]. Readers unfamiliar to association schemes should refer to that source.

Let X be a finite dimensional linear space over F_2 and X' its dual space, and let $\langle .\,,.\rangle : X \times X' \to F_2$ denote the bilinear pairing between X and X'. For a subset $Y \subset X$ the annihilator $Y^0 \subset X'$ is defined by

$$Y^0 = \{y' \in X' \mid \langle y, y'\rangle = 0 \; \forall_{y \in Y}\}.$$

Note that for a linear subspace $Y \subset X$

$$\sum_{y \in Y} (-1)^{\langle y, x'\rangle} = \begin{cases} |Y|, & \text{if } x' \in Y^0 \\ 0, & \text{if } x' \notin Y^0. \end{cases}$$

In particular

$$\sum_{x \in X} (-1)^{\langle x, x'\rangle} = v \cdot \delta_{0x'},$$

where $v = |X|$ denotes the cardinality of X.

Now let $\mathcal{G}$ be a subgroup of $\mathrm{Aut}(X)$, the automorphism group of the linear space X. Set $\mathcal{G}' := \{g' \in \mathrm{Aut}(X') \mid g \in \mathcal{G}\}$, where g' is defined via the identity $\langle gx, x'\rangle = \langle x, g'x\rangle$ for all $x \in X$, $x' \in X'$. The two groups are of course isomorphic, where an isomorphism is given by $g \mapsto (g^{-1})'$.

$\mathcal{G}$ and $\mathcal{G}'$ can be used to define a pair of association schemes $(X, \mathcal{R})$ and $(X', \mathcal{R}')$ on X and X' respectively, which we will call linear. Let $C_0, C_1, \ldots, C_d$ be the orbits in X under the action of $\mathcal{G}$, where $C_0 = \{0\}$. Then these $d+1$ classes define a set $\mathcal{R} = \{R_0, R_1, \ldots, R_d\}$ of $d+1$ symmetric relations $R_i \subset X \times X$, with $(x, y) \in R_i$ iff $x + y \in C_i$. The incidence matrix of the relation R_i will be denoted by D_i. This defines an association scheme $(X, \mathcal{R})$. Analogously we define the association scheme $(X', \mathcal{R}')$ on X', where the set of relations $\mathcal{R}' = \{R_0', R_1', \ldots, R_d'\}$ arises from the orbits $C_0', C_1', \ldots, C_d'$ in X' under the action of $\mathcal{G}'$. The elements, classes, incidence matrices and idempotents of $(X', \mathcal{R}')$ will all be marked with a ', i.e. x', C_i', D_i', J_i'.

It turns out that the linear association schemes defined above form a dual pair (for a definition see [2]), and that their eigenvalues can be given explicitly.

Theorem 3. *The linear association schemes $(X, \mathcal{R})$ and $(X', \mathcal{R}')$ are dual to each other. The primitive idempotent J_k $(k = 0, \ldots, d)$ of $(X, \mathcal{R})$ is the matrix with*

(x, y)th *entry*

$$\frac{1}{v}\sum_{z'\in C_k'}(-1)^{\langle x+y,z'\rangle}.$$

The eigenvalues are given by

$$q_k(i)=\sum_{z'\in C_k'}(-1)^{\langle x,z'\rangle} \quad \textit{with } x\in C_i, \textit{ and}$$

$$p_k(i)=\sum_{z\in C_k}(-1)^{\langle z,x'\rangle} \quad \textit{with } x'\in C_i'.$$

We will sketch the proof in Lemmas 1 to 4 below, closely following the proof of Theorem 5, Ch. 21 in [7]. The fact that $(X, \mathcal{R})$ and $(X', \mathcal{R}')$ are dual association schemes is then an immediate consequence of the expressions for $p_k(i)$, $q_k(i)$ given above, since exchanging the classes $C_i \leftrightarrow C_i'$ yields the dual definitions.

Lemma 1. *The numbers $p_k(i)$, $q_k(i)$ are independent of the particular choice of $x\in C_i$, $x'\in C_i'$ respectively.*

Proof. We will show this for $q_k(i)$. Let $\tilde{x}$ be any other element of class C_i. Then there exists an element $g\in\mathcal{G}$ such that $\tilde{x}=gx$. Hence

$$\sum_{z'\in C_k'}(-1)^{\langle \tilde{x},z'\rangle}=\sum_{z'\in C_k'}(-1)^{\langle gx,z'\rangle}$$

$$=\sum_{z'\in C_k'}(-1)^{\langle x,g'z'\rangle}=\sum_{z'\in C_k'}(-1)^{\langle x,z'\rangle},$$

where the last equality comes from the fact that $g\in\mathcal{G}$ implies $g'\in\mathcal{G}'$ and thus g' only induces a permutation of the elements in C_k'. □

In the next step we will show that the matrices J_k can be obtained as

$$J_k=\frac{1}{v}\sum_{i=0}^{d}q_k(i)D_i,$$

thus J_k belongs to the Bose–Mesner algebra of the association scheme. Then we prove that the J_ks are indeed the primitive idempotents of this algebra.

Lemma 2.

$$(J_k)_{xy}=\frac{1}{v}\sum_{z'\in C_k'}(-1)^{\langle x+y,z'\rangle}=\frac{1}{v}\sum_{i=0}^{d}q_k(i)(D_i)_{xy}.$$

Proof. Let $x+y\in C_{i_0}$. Then $(D_i)_{xy}=1$ iff $i=i_0$.

$$\frac{1}{v}\sum_{i=1}^{d}q_k(i)(D_i)_{xy}=\frac{1}{v}q_k(i_0)=\frac{1}{v}\sum_{z'\in C_k'}(-1)^{\langle x+y,z'\rangle}=(J_k)_{xy}. \quad \square$$

Lemma 3. *The J_k are primitive idempotents, i.e. $J_i^2 = J_i$, $J_iJ_k = 0$ for $i \neq k$.*

Proof.

$$\begin{aligned}(J_iJ_k)_{xy} &= \sum_{w\in X} (J_i)_{xw}\cdot(J_k)_{wy}\\ &= \frac{1}{v^2}\sum_{w\in X}\Big(\sum_{r'\in C_i'}(-1)^{\langle x+w,r'\rangle}\Big)\cdot\Big(\sum_{s'\in C_k'}(-1)^{\langle w+y,s'\rangle}\Big)\\ &= \frac{1}{v^2}\sum_{r'\in C_i'}\sum_{s'\in C_k'}\sum_{w\in X}(-1)^{\langle x+w,r'\rangle+\langle w+y,s'\rangle}\\ &= \frac{1}{v^2}\sum_{r'\in C_i'}\sum_{s'\in C_k'}(-1)^{\langle x,r'\rangle+\langle y,s'\rangle}\cdot\sum_{w\in X}(-1)^{\langle w,r'+s'\rangle}\\ &= \frac{1}{v^2}\sum_{r'\in C_i'}\sum_{s'\in C_k'}(-1)^{\langle x,r'\rangle+\langle y,s'\rangle}\cdot v\delta_{r's'}.\end{aligned}$$

Therefore $(J_i\cdot J_j)_{xy} = 0$ if $i\neq k$, since then $r'\neq s'$ and thus $\delta_{r's'}=0$. If $i=k$, we have

$$(J_k)_{xy}^2 = \frac{1}{v^2}\sum_{r'\in C_i'}(-1)^{\langle x+y,r'\rangle}\cdot v = (J_k)_{xy}. \quad \square$$

We know now that $Q=(q_{ij})$ with $q_{ij}=q_j(i)$ is one eigenmatrix of the association scheme. We will show that $P=(p_{ij})$ with $p_{ij}=p_j(i)$ is the other eigenmatrix by showing that $P\cdot Q = vI$.

Lemma 4. *Let v_k denote the cardinality of C_k, and w_k the cardinality of C_k'. Then*

(i) $v_iq_k(i) = w_kp_i(k)$

(ii) $\sum_{i=0}^{d} v_iq_k(i)q_r(i) = vw_k\delta_{kr}$

(iii) $P\cdot Q = v\cdot I$.

Proof. We will only prove (ii) here. (i) is easy to show, and (iii) follows using (i) and (ii);

$$\begin{aligned}\sum_{i=0}^{d} v_iq_k(i)q_r(i) &= \sum_{i=0}^{d}\sum_{x\in C_i}\Big(\sum_{y'\in C_k'}(-1)^{\langle x,y'\rangle}\cdot\sum_{z'\in C_r'}(-1)^{\langle x,z'\rangle}\Big)\\ &= \sum_{y'\in C_k'}\sum_{z'\in C_r'}\sum_{x\in X}(-1)^{\langle x,y'+z'\rangle}\\ &= \sum_{y\in C_k'}\sum_{z'\in C_r'} v\cdot\delta_{z'y'}.\end{aligned}$$

If $k\neq r$, then $z'\neq y'$ and thus the above sum is 0. If $k=r$, then

$$\sum_{y'\in C_k'}\sum_{z'\in C_k'} v\cdot\delta_{z'y'} = \sum_{y'\in C_k'} v = v\cdot w_k. \quad \square$$

This concludes the proof of Theorem 3.

For a nonempty subset $Y \subset X$ the class distribution of Y with respect to the association scheme $(X, \mathcal{R})$ is the $(d+1)$-tuple $\boldsymbol{c}(Y) = (c_0, \ldots, c_d)$, where c_i is the number of $y \in Y$ which belong to class C_i. The inner distribution of the subset Y is the $(d+1)$-tuple $\boldsymbol{b}(Y) = (b_0, \ldots, b_d)$, where

$$b_i := \frac{1}{|Y|} |R_i \cap Y^2|$$

is the average number of $z \in Y$ which are ith associates of a point $y \in Y$. For a linear subset Y we have of course $\boldsymbol{c}(Y) = \boldsymbol{b}(Y)$.

Delsarte [2] proved that the transforms b_i' of an inner distribution have always to be nonnegative. His theorem can be used to derive a bound on the cardinality of subsets Y with certain restrictions on their inner distribution (see Theorem 8):

Theorem 4 (Delsarte). *Let $\boldsymbol{b} = (b_0, \ldots, b_d)$ be the inner distribution of a nonempty subset $Y \subset X$. Then*

$$b_k' = \frac{1}{|Y|} \sum_{i=0}^{d} b_i \cdot q_k(i) \geqslant 0$$

for $k = 0, \ldots, d$, where the $q_k(i)$s are the eigenvalues of the association scheme.

The duality of a linear subspace $Y \subset X$ and its annihilator $Y^0 \subset X'$ is reflected by the duality of the association schemes. We have the following result, which follows from (6.9) in [2].

Theorem 5. *Let Y be a linear subspace of X and $Y^0 \subset X'$ its annihilator. Then the inner distribution $\boldsymbol{b}'(Y^0) = (b_0', \ldots, b_d') \in R^{d+1}$ of Y^0 in $(X', \mathcal{R}')$ is the dual distribution of the inner distribution $\boldsymbol{b}(Y) = (b_0, \ldots, b_d) \in R^{d+1}$ of Y in $(X, \mathcal{R})$:*

$$\boldsymbol{b}'(Y^0) = \frac{1}{|Y|} \boldsymbol{b}(Y) \cdot Q, \qquad \boldsymbol{b}(Y) = \frac{1}{|Y^0|} \boldsymbol{b}(Y^0) \cdot P.$$

The transformation $\boldsymbol{b}(Y) \mapsto (1/|Y|)\boldsymbol{b}(Y) \cdot Q$ can of course be also applied to the inner distribution of a nonlinear subset $Y \subset X$. If there exists a subset $Y' \subset X'$, with the property that $\boldsymbol{b}'(Y') = (1/|Y|)\boldsymbol{b}(Y) \cdot Q$, then Y and Y' are called formal duals.

The best known example of the previous theorem is of course the MacWilliams duality in the Hamming association scheme. In this case we choose as $\mathcal{G} \subset \mathrm{GL}(n, 2)$ the roup of all $n \times n$-permutation matrices acting on $X = F_2^n$. Denote by

$$(.\,,.) : F_2^n \times F_2^n \to F_2$$

the usual scalar product on F_2^n. Then we can identify the dual space X' with X using $(.\,,.)$ as the bilinear pairing. Then $\mathcal{G}' = \mathcal{G}^{\mathrm{T}} = \mathcal{G}$ and the elements of the classes $C_k = C_k'$ with $0 \leqslant k \leqslant n$ are the vectors of weight k, which defines the selfdual Hamming association scheme. The annihilator Y^0 of a linear subspace

(code) $Y \subset F_2^n$ is then the dual code

$$Y^\perp = \{x \in F_2^n \mid (x, y) = 0 \; \forall_{y \in Y}\},$$

and the inner distributions are the distance distributions of the respective codes.

3. Linear association schemes on quotient spaces

We will now consider dual pairs of linear association schemes on certain quotient spaces in F_2^n and their interplay with the Hamming association scheme on F_2^n.

Let A and B be two binary linear codes (subspaces) of length n with $B \subset A \subset F_2^n$. Consider the quotient F_2-spaces

$$X := A/B \quad \text{and} \quad X' := B^\perp/A^\perp.$$

For an element $a \in A$ denote by $[a] \in X$ the coset $a + B$. Accordingly for $b' \in B^\perp$ define $[b'] \in X'$ to be the coset $b' + A^\perp$. X' is naturally interpreted as the dual space of X by defining the bilinear pairing canonically as

$$\langle [x], [x'] \rangle := (x, x'),$$

where $(.\,,.) : F_2^n \times F_2^n \to F_2$ again denotes the scalar product on F_2^n. Now let $\mathcal{G}$ be an automorphism group of the code A that preserves the subcode B. Consider the natural action of $\mathcal{G}$ on the quotient space X: for $g \in \mathcal{G}$ let $[x]^g := [gx]$. Thus $\mathcal{G}$ is a subgroup of $\mathrm{Aut}(X)$ and hence $\mathcal{G}$ induces a dual pair of linear association schemes $(X, \mathcal{R})$ and $(X', \mathcal{R}')$ on X and X' as shown in Theorem 3.

What we want to show is the fact that the duality of subsets in the association schemes $(X, \mathcal{R})$ and $(X', \mathcal{R}')$ carries over to the duality of certain codes in the Hamming association scheme. Let Y be a nonempty subset of $X = A/B$. We define the code

$$C_Y := \bigcup_{[y] \in Y} (y + B),$$

i.e. C_Y is a union of cosets of B with coset representatives y, where $[y] \in Y \subset X$. In the same way we define the code $C_{Y'}$ for a nonempty subset $Y' \subset X' = B^\perp/A^\perp$ as

$$C_{Y'} := \bigcup_{[y'] \in Y'} (y' + A^\perp).$$

Since $\langle [y], [y'] \rangle := (y, y')$, it follows immediately that for a linear subspace $Y \subset X$ with annihilator $Y^0 \subset X'$

$$C_Y^\perp = C_{Y^0}.$$

For a code $C \subset F_2^n$ let $w(C) = (w_0, \ldots, w_n) \in R^{n+1}$ denote its weight distribution, i.e. the class distribution of C in the Hamming scheme on F_2^n. Since by

assumption $\mathcal{G}$ is a subgroup of the automorphism groups of the codes A and B, the weight distribution of a coset $a_i + B$ with $[a_i] \in C_i$ depends only on the class C_i of the association scheme $(X, \mathcal{R})$. For $0 \leq i \leq d$ and $0 \leq j \leq n$ denote by t_{ij} the number of vectors of weight j in the cosets $a_i + B$. This defines a $(d+1) \times (n+1)$-matrix $T = (t_{ij})$ (the ith row is the weight distribution $w(a_i + B)$ of the coset $a_i + B$). Analogously we define the matrix $T' = (t'_{ij})$ where t'_{ij} is the number of vectors of weight j in the coset $b'_i + A^{\perp}$, where $[b'_i] \in C'_i$.

Let $c(Y)$, $c'(Y') \in R^{d+1}$ denote again the class distribution of Y in $(X, \mathcal{R})$, and Y' in $(X', \mathcal{R}')$ respectively. Then we have

$$w(C_Y) = c(Y) \cdot T, \quad \text{and } w(C_{Y'}) = c'(Y') \cdot T'.$$

Denote by $M = (m_{ij})$ the real $(n+1) \times (n+1)$-eigenmatrix of the selfdual Hamming association scheme, i.e. $m_{ij} = P_j(i)$, where $P_j(i)$ is the value of the Krawtchouk polynomial $P_j(x) = \sum_{k=0}^{j} (-1)^k \binom{x}{k} \binom{n-x}{j-k}$ at i (see Ch. 21 [7]).

Lemma 5. *With T, T', P, Q, M defined as above:*

$$Q \cdot T' = \frac{1}{|B|} T \cdot M \qquad P \cdot T = \frac{1}{|A^{\perp}|} T' \cdot M.$$

Proof. Let Y be a linear subset of X, then we know from Theorem 5 that the class distribution of the annihilator Y^0 is the dual of the class distribution of Y. Furthermore we have seen that for linear Y, the codes C_Y and C_{Y^0} are dual to each other, and thus their weight distributions are linked via the MacWilliams transformation; i.e. we have

$$\frac{1}{|Y|} c(Y) \cdot Q \cdot T' = c'(Y^0) \cdot T' = w(C_{Y^0})$$

$$= w(C_Y^{\perp}) = \frac{1}{|C_Y|} w(C_Y) \cdot M = \frac{1}{|C_Y|} c(Y) \cdot T \cdot M.$$

Hence for any linear subspace $Y \subset X$ we get

$$\frac{1}{|Y|} c(Y) \cdot Q \cdot T' = \frac{1}{|C_Y|} c(Y) \cdot T \cdot M,$$

or using $|C_Y| = |B| \cdot |Y|$

$$c(Y) \cdot Q \cdot T' = \frac{1}{|B|} c(Y) \cdot T \cdot M$$

for every $c(Y) \in R^{d+1}$ which comes from a linear subspace $Y \subset X$. If we choose as linear subspaces $Y_i := \{[0], [a_i]\}$, with $a_i \in C_i$, the corresponding class distributions $c(Y_i)$ span a basis of R^{d+1}. This shows that

$$Q \cdot T' = \frac{1}{|B|} T \cdot M. \quad \square$$

As a consequence of Lemma 5 we have

Theorem 6. *Let $Y \subset X$ have a (formal) dual $Y' \subset X'$. Then the corresponding codes C_Y, $C_{Y'} \subset F_2^n$ are (formal) duals in the Hamming association scheme – their weight (distance) distributions are MacWilliams transforms of each other.*

It is not difficult to prove a more general version of Theorem 6. Start with a dual pair of linear association schemes $(Z, \mathcal{S})$, $(Z', \mathcal{S}')$ induced by a group $\mathcal{H} \subset \mathrm{Aut}(Z)$ on the linear spaces Z and Z' (in the theorem above, the selfdual Hamming association scheme played the role of the dual pair, where $\mathcal{H}$ would be the group of all $n \times n$-permutation matrices acting on $Z = Z' = F_2^n$ – see remark after Theorem 5). Let $B \subset A \subset Z$ be two linear subspaces of Z and define $X = A/B$, $X' = B^0/A^0$ with the canonical bilinear pairing derived from the bilinear form on $Z \times Z'$.

Now let $\mathcal{G} \subset \mathcal{H}$ be a subgroup of $\mathcal{H}$, which is also an automorphism group of A and B. Then $\mathcal{G}$ defines a dual pair of association schemes $(X, \mathcal{R})$ and $(X', \mathcal{R}')$ on the quotient spaces X and X'. For $Y \subset X$ and $Y' \subset X'$ set

$$C_Y := \bigcup_{[y] \in Y} (y + B) \subset Z \qquad C_{Y'} := \bigcup_{[y'] \in Y'} (y' + A^0) \subset Z',$$

and we get:

Theorem 7. *With the notation given above, let $Y \subset X$ have a (formal) dual $Y' \subset X'$ in the pair of association schemes $(X, \mathcal{R})$ and $(X', \mathcal{R}')$, then the corresponding subsets $C_Y \subset Z$ and $C_{Y'} \subset Z'$ are (formal) duals with respect to the association schemes $(Z, \mathcal{S})$ and $(Z', \mathcal{S}')$.*

4. The association schemes on quotients of Reed–Muller codes

We can now apply our results from the previous section to the family of Reed–Muller codes (see Ch. 13 in [7]). Let $V_m := F_2^{2^m}$. For $0 \leq r \leq m$ the Reed–Muller codes $\mathrm{RM}(r, m) \subset V_m$ form a family of nested linear codes of length 2^m

$$\mathrm{RM}(0, m) \subset \mathrm{RM}(1, m) \subset \cdots \subset \mathrm{RM}(m-1, m) \subset \mathrm{RM}(m, m).$$

The dual of the rth order RM-code $\mathrm{RM}(m, r)$ is $\mathrm{RM}(m-r-1, r)$. Furthermore these codes share the same automorphism group. In particular, for all $0 \leq r \leq m$, $\mathrm{Aut}(\mathrm{RM}(r, m))$ contains a group $\mathcal{G} \subset \mathrm{GL}(2^m, 2)$, which is isomorphic to $\mathrm{GL}(m, 2)$.

Thus we can apply Theorem 6 and immediately have the following result.

Lemma 6. *The linear association schemes $(X, \mathcal{R})$ and $(X', \mathcal{R}')$ induced by $\mathcal{G}$ on*

$$X := \mathrm{RM}(r, m)/\mathrm{RM}(r-1, m) \quad \textit{and}$$
$$X' := \mathrm{RM}(m-r, m)/\mathrm{RM}(m-r-1, m)$$

are dual to each other. Furthermore, if $Y \subset X$ has a (formal) duals $Y' \subset X'$, then the corresponding codes in V_m

$$C_Y = \bigcup_{[y] \in Y} (y + \mathrm{RM}(r-1, m)) \quad \textit{and} \quad C_{Y'} = \bigcup_{[y'] \in Y'} (y' + \mathrm{RM}(m-r-1, m))$$

are (formal) duals in the Hamming association scheme.

This is the key lemma to derive the result on Delsarte–Goethals codes and their formal duals (Theorem 2). In the remainder of this section we will show that the two association schemes are actually isomorphic, or equivalently that $(X, \mathcal{R})$ is selfdual, and define the isomorphism $\alpha: V_m \to V_m$ that maps the coset representatives of a DG-code onto the coset representatives of the corresponding GD-code.

Reed–Muller codes can be defined very simply in terms of polynomials over F_2. Let X_m denote the 2^m-dimensional F_2-space consisting of all linear combinations of the 2^m squarefree polynomials in m variables. Let X_m^r be the $\binom{m}{r}$-dimensional subspace generated by all monomials of degree r, thus

$$X_m = X_m^0 \oplus X_m^1 \oplus \cdots \oplus X_m^{m-1} \oplus X_m^m.$$

Indexing the coordinates of V_m with the 2^m vectors in F_2^m gives a natural interpretation of V_m as the linear space of all boolean functions $f: F_2^m \to F_2$. Furthermore every such boolean function has a unique representation as a polynomial in X_m. Thus there exists an isomorphism $\Phi: X_m \to V_m$, and therefore we will identify the spaces V_m and X_m. Whenever we refer to the weight distribution of a code $C \subset X_m$, we mean of course its weight distribution as a subset of V_m.

In this manner the rth order Reed–Muller code can simply be defined as

$$\mathrm{RM}(r, m) = X_m^0 \oplus X_m^1 \oplus \cdots \oplus X_m^r,$$

and

$$X_m^r = \mathrm{RM}(r, m)/\mathrm{RM}(r-1, m).$$

In the sequel we will denote the dual pair of linear association schemes from Lemma 6 induced by $\mathcal{G}$ on X_m^r and X_m^{m-r} by $(X_m^r, \mathcal{R}_m^r)$ and $(X_m^{m-r}, \mathcal{R}_m^{m-r})$. The subgroup $\mathcal{G}$ of the automorphism group of the Reed–Muller codes can be represented as the group $\mathrm{GL}(m, 2)$ acting on X_m by applying a matrix $A \in \mathrm{GL}(m, 2)$ to the arguments of a polynomial $p(v_1, \ldots, v_m) \in X_m$. E.g. let

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}(3, 2) \quad \text{and } p(v_1, v_2, v_3) = v_1 v_2 + v_2 v_3 \in X_3.$$

Then

$$\begin{aligned} p(v)^A &= p(A(v)) = p(v_1, v_2, v_1 + v_2 + v_3) \\ &= v_1 v_2 + v_2(v_1 + v_2 + v_3) = v_1 v_2 + v_1 v_2 + v_2 v_3 + v_2 = v_2 v_3 + v_2. \end{aligned}$$

Choose the $\binom{m}{r}$ monomials of degree r as the basis of X_m^r. Then it is not difficult to check that with respect to this basis the action of $\mathcal{G}$ on X_m^r is represented by a matrix group

$$\mathcal{G}_m^r \subset \mathrm{GL}\left(\binom{m}{r}, 2\right),$$

which is closed under transposition, i.e. $A \in \mathcal{G}_m^r$ implies $A^{\mathrm{T}} \in \mathcal{G}_m^r$. If we now choose the dual basis for X_m^{m-r}, then the action of $\mathcal{G}$ on X_m^{m-r} is represented by the group

$$\mathcal{G}_m^{m-r} = (\mathcal{G}_m^r)' = (\mathcal{G}_m^r)^{\mathrm{T}} = \mathcal{G}_m^r.$$

Hence the mapping $\alpha: X_m^r \to X_m^{m-r}$, which maps the basis of X_m^r onto its dual basis in X_m^{m-r}, defines a linear isomorphism between the dual pair of linear association schemes $(X_m^r, \mathcal{R}_m^r)$ and $(X_m^{m-r}, \mathcal{R}_m^{m-r})$; or in other words, the linear association scheme $(X_m^r, \mathcal{R}_m^r)$ is selfdual.

α is of course the linear isomorphism on X_m, which maps a monomial $\prod_{i \in N} v_i$ with $N \subset M = \{1, \ldots, m\}$ to its "complement"

$$\alpha\left(\prod_{i \in N} v_i\right) = \prod_{j \in M-N} v_j.$$

This is the bijection between the coset leaders of a DG(m, j) and GD(m, j)-code used in Theorem 2 (interpreting the coset leaders as elements of X_m^2 and X_m^{m-2} respectively). We can now rephrase Lemma 6 in the following way:

Lemma 6a. *Let Y be a subset of X_m^r which has a (formal) dual $Z \subset X_m^r$ in the selfdual association scheme $(X_m^r, \mathcal{R}_m^r)$. Then the codes*

$$C_Y = \bigcup_{y \in Y} (y + \mathrm{RM}(r-1, m)) \quad \textit{and} \quad C_Z = \bigcup_{z \in Z} (z + \mathrm{RM}(r-1, m))$$

have formal duals $C_Y' = C_{\alpha(Z)}$ and $C_Z' = C_{\alpha(Y)}$ respectively:

$$C_Y' = C_{\alpha(Z)} = \bigcup_{z \in Z} (\alpha(z) + \mathrm{RM}(m-r-1, m))$$

and

$$C_Z' = C_{\alpha(Y)} = \bigcup_{y \in Y} (\alpha(y) + \mathrm{RM}(m-r-1, m)).$$

In other words, the coset leaders of the dual of C_Y are the images under α of the coset leaders of C_Z, and the coset leaders of the dual of C_Z are the images of the coset leaders of C_Y.

5. The DG-codes and their duals in the GD-codes

Delsarte and Goethals defined the DG-codes using the association scheme of symplectic forms, which is isomorphic to $(X_m^2, \mathcal{R}_m^2)$: Every homogeneous polynomial $p(v_1, \ldots, v_m) \in X_m^2$ defines a binary symplectic matrix $S = (s_{ij})$, where $s_{ij} = s_{ji} = 1$ iff $v_i v_j$ is a monomial of $p(v_1, \ldots, v_m)$. It turns out that two polynomials $p, q \in X_m^2$ are in the same class C of the association scheme, iff their corresponding symplectic matrices have the same rank. So $(X_m^2, \mathcal{R}_m^2)$ is the symplectic association scheme with $m/2$ classes, and $p \in C_i$, iff the associated symplectic matrix S has $\operatorname{rank}(S) = 2i$ [3]. Furthermore the minimum weight in the coset $p + \mathrm{RM}(1, m) \subset V_m$ with $p \in C_i$ is $2^{m-1} - 2^{m-1-i}$.

A subset $Y \in (X_m^2, \mathcal{R}_m^2)$ is called an (m, d)-set, if every nonzero polynomial in Y belongs to a class C_i with $i \geq d$ and the sum of any two distinct elements $p, q \in Y$ also belongs to a class C_i with $i \geq d$, i.e. an (m, d)-set Y has an inner distribution $\boldsymbol{b}(Y) = (b_0, \ldots, b_{m/2})$ with $b_j = 0$ for $0 < j < d$.

Given an (m, d)-set Y, the code

$$C_Y := \bigcup_{p \in Y} (p + \mathrm{RM}(r-1, m))$$

has minimum distance $2^{m-1} - 2^{m-1-d}$. A Delsarte–Goethals code $\mathrm{DG}(m, d)$ is then defined to be the code C_Y for a maximal (m, d)-set Y.

Delsarte and Goethals were able to construct maximal (m, d)-sets and to prove their maximality using Theorem 4. The following theorem summerizes their results on these sets [3]:

Theorem 8. *For even $m = 2t$ and $1 \leq d \leq \frac{1}{2}m$, the maximum cardinality of an (m, d)-set $Y(m, d) \subset X_m^2$ is*

$$2^k \quad \textit{where } k = (m-1)(t-d+1).$$

Furthermore the inner distribution of a maximal $Y(m, d)$ is completely determined by the parameters (m, d). The inner distribution of $Y(m, j)$

$$\boldsymbol{b}'(Y(m, j)) = (b_0', \cdots, b_{m/2}')$$

is the transform of the inner distribution of $Y(m, d)$

$$\boldsymbol{b}(Y(m, d)) = (b_0, \cdots, b_{m/2})$$

with $j + d = m/2 + 2$; i.e. $Y(m, d)$ and $Y(j, d)$ are formal duals in $(X_m^2, \mathcal{R}_m^2)$.

We are now ready to prove Theorem 2.

Proof of Theorem 2. Since for $d + j = \frac{1}{2}m + 2$ the sets $Y(m, d)$, $Y(m, j) \subset X_m^2$ are formal duals in $(X_m^2, \mathcal{R}_m^2)$ (Theorem 8), Lemma 6a tells us that the code

$$\mathrm{DG}(m, j) := C_{Y(m,j)} = \bigcup_{p \in Y(m,j)} (p + \mathrm{RM}(1, m))$$

is a formal dual of the code GD(m, d) defined by

$$\mathrm{GD}(m, d) := \bigcup_{q \in Y(m,d)} (\alpha(q) + \mathrm{RM}(m-3, m)).$$

Furthermore the DG- and GD-codes are distance invariant since the inner distribution of a maximal (m, d)-set is unique. □

6. Are there good generalizations of the DG-codes?

There is an obvious way to generalize the definition of (m, d)-sets and DG-codes: We take the linear association scheme $(X_m^r, \mathscr{R}_m^r)$. Number the classes $C_0, \cdots, C_s$ in such a way, that $w_i^r \leq w_{i+1}^r$, where w_i^r is the minimum weight of the coset $p + \mathrm{RM}(r-1, m)$ for a representative $p \in C_i$. Then define an (m, r, d)-set $Y \subset X_m^r$ analogously to an (m, d)-set $\subset X_m^2$ (an (m, d)-set then becomes an (m, 2, d)-set), and define an XDG(m, r, d)-code to be the code

$$\mathrm{XDG}(m, r, d) = C_Y = \bigcup_{p \in Y} p + \mathrm{RM}(r-1, m),$$

where Y is a maximal (m, r, d)-set. The minimum distance of XDG(m, r, d) is w_d^r.

With this notation a DG(m, d)-code becomes an XDG(m, 2, d)-code and a GD(m, d)-code becomes an XDG(m, $m-2$, d)-code. Of course the difficulty is to come up with a maximal (m, r, d)-set. Moreover in the general case (for $r \neq 2$, $m-2$) there does not seem to exist such a nice characterization of the classes C_i of $(X_m^r, \mathscr{R}_m^r)$.

The smallest interesting case would be $m = 6$, $r = 3$. The original intention of this work was the construction of XDG(6, 3, d)-codes, but so far we did not succeed. On the other hand, the bounds on maximal (6, 3, d)-sets obtained from the linear association scheme $(X_6^3, \mathscr{R}_6^3)$ are very promising. We want to end this paper with some results about this association scheme and their implications for possible XDG(6, 3, d)-codes.

Lemma 7. *The linear association scheme* $(X_6^3, \mathscr{R}_6^3)$ *has* 6 *classes* $C_0, \ldots, C_5$. *Representatives of the classes are given in Fig. 1. The eigenmatrices* $P = (p_{ik})$ *with* $p_{ik} = p_k(i)$, $0 \leq i, k \leq 5$ *is*

$$\begin{pmatrix} 1 & 1395 & 54684 & 357120 & 468720 & 166656 \\ 1 & 371 & 4508 & 4864 & -4368 & -5376 \\ 1 & 115 & 156 & -1280 & 240 & 768 \\ 1 & 19 & -196 & 512 & -336 & 0 \\ 1 & -13 & 28 & -256 & 496 & -256 \\ 1 & -45 & 252 & 0 & -720 & 512 \end{pmatrix}$$

i	$\lvert C_i\rvert$	representative $p(x)$
0	1	$p(x)=0$
1	1395	$p(x)=x_1x_2x_3$
2	54684	$p(x)=x_1(x_2x_3+x_4x_5)$
3	357120	$p(x)=x_1x_2x_3+x_4x_5x_6$
4	468720	$p(x)=x_1x_2x_4+x_1x_3x_5+x_2x_3x_6$
5	166656	$p(x)=x_1x_3x_5+x_1x_3x_6+x_1x_4x_6+x_2x_3x_6+x_2x_4x_5$

Fig. 1.

i	0/64	8/56	12/52	14/50	16/48	18/46	20/44	22/42	24/40	26/38	28/36	30/34	32
0	1	—	—	—	2604	—	—	—	291648	—	888832	—	1828134
1	—	8	—	—	784	—	14336	—	241528	—	989184	—	1702624
2	—	—	32	—	384	—	17312	—	230912	—	1010752	—	1675520
3	—	—	—	64	—	3136	—	73472	—	546560	—	1473920	—
4	—	—	—	—	448	—	17920	—	227584	—	1018368	—	1665664
5	—	—	—	—	—	3584	—	72192	—	548352	—	1473024	—

Fig. 2. Weight distribution of the cosets $p + \mathrm{RM}(2, 6)$, for $p \in C_i$, $0 \leq i \leq 5$. Since the all-ones vector is in RM(2, 6), the number of codewords of weight w is equal to the number of vectors of weight $64 - w$, the entry in column $w/(64 - w)$ gives this number.

d	$\lvert(6, 3, d)$-set$\rvert$	$\lvert\mathrm{XDG}(6, 3, d)\rvert$	min dist
2	2^{15}	2^{22+15}	12
3	2^{10}	2^{22+10}	14
5	2^{5}	2^{22+5}	16

Fig. 3. Table of bounds for XDG(6, 3, d)-codes. The XDG(6, 3, d)-codes are all of length 64. Since they are unions of cosets of RM(3, 6) their cardinalities are multiples of $\lvert\mathrm{RM}(3, 6)\rvert = 2^{22}$.

The weight distributions of the cosets $p + \mathrm{RM}(6, 3)$ are given in *Fig. 2.*

Using Theorem 4 we can derive upper bounds for the cardinalities of (6, 3, d)-sets. The situation is similar to the case $r = 2$ but a little more irregular.

Of course XDG(6, 3, 1) is RM(3, 6). If there are maximal (6, 3, d)-sets which meet the bounds given by the association scheme (X_6^3, G_6^3), the XDG(6, 3, 2)-code would have as a formal dual the XDG(6, 3, 5)-code. Furthermore there would exist a formally self dual XDG(6, 3, 3)-code. But in contrast to the case $r = 2$ the inner distribution of this code is not uniquely determined by the association scheme. All these codes would be better than the best codes known to exist. *Fig. 3* gives the cardinalities and minimum distances of these hypothetical codes.

Acknowledgement

I thank the anonymous referee for some very helpful suggestions concerning linear association schemes on quotient spaces.

References

[1] R.D. Baker, J.H. van Lint and R.M. Wilson, On the Preparata and Goethals codes, IEEE Trans. Inform. Theory IT-29 (5) (1983) 342–345.
[2] P. Delsarte, An algebraic approach to the asociation schemes of coding theory, Philips Res. Rep. Suppl. 10 (1973).
[3] P. Delsarte and J.-M. Goethals, Alternating bilinear forms over GF(q), J. Combin. Theory 19A (1975) 211–224.
[4] J.-M. Goethals, Two dual families of nonlinear binary codes, Electronic Letters 10 (1974) 471–472.
[5] J.-M. Goethals, Nonlinear codes defined by quadratic forms over GF(2), Inform. and Control 31 (1976) 43–74.
[6] A.M. Kerdock, A class of low-rate nonlinear codes, Inform. and Control 20 (1972) 182–187.
[7] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, New York, 1981).
[8] F.P. Preparata, A class of optimum nonlinear double-error correcting codes, Inform. and Control 13 (1968) 378–400.